MALWARE CLASSIFICATION USING DEEP LEARNING

Ameena K Nazeer
Department of Computer Science and Engineering
College of Engineering Trivandrum
amoosameena@gmail.com

Thara R.J.
Department of Computer Science and Engineering
College of Engineering Trivandrum
tharaneelima@cet.ac.in

***Abstract*—As new technological era begins in the field of information technology that transfer human existence from real to computerized world, malware, or malicious software, is a huge threat to the information technology world.The field of Deep Learning have recently shown to be more effective at identifying and categorising malware.Here,the paper proposed new methods using deep neural networks for the classification of malware images into its respective classes. In the creation of those algorithms, feature engineering is a critical stage. This takes an excessive amount of time. Using deep learning techniques, this move can be completely prevented. According to recent research, many of them used skewed data collecting, which is completely worthless in real-time situations. As a result, a new method / architecture to identify malware using deep learning is being developed.Using sophisticated Convolutional Neural Networks and the weight sharing concept to find patterns in malware sequences. By combining this with Recurrent Neural Networks, we may be able to detect reoccurring malware trends.**

***Index Terms*—Deep Learning,Convolutional Neural Network, Recuurent Neural Network, Support Vector Machine.**

I. INTRODUCTION

Malware is a serious danger to computer users' security and can result in large financial losses for businesses. As the Internet of Things (IoT) has grown in popularity, attackers have begun to target it. Malware is known by a variety of names, including adware, rootkits, backdoors, ransomware, trojans, worms, spyware, and so on, depending on its behaviour. As a result, detecting these malwares has become a growing difficulty for researchers. The two forms of malware analysis and detection processes are static analysis and dynamic analysis. The process of studying and extracting information from an executable file without running it is known as static analysis. The process of running malware and studying its behaviour on the system is known as dynamic analysis.Experts will either manually test the sample with a new type of malware or build a programme to compare the malware similarity. Image classification has recently improved considerably thanks to advances in deep learning algorithms. Other forms of neural networks were outperformed by convolutional neural networks. Feature engineering, feature learning, and feature representation are all automated in this application.

Static Malware Analysis (SMA) is a fundamental malware analysis method that does not require the malware to be executed. Different SMA methodologies includes Basic Information Analysis, PE File Structure Analysis, and Control Flow Analysis .The increase in the number of malwares use techniques like Shell Code, Polymorphism, and Metamorphism makes malware analysis,detection and classification more difficult.

To avoid the disruptions of Shell Code, Polymorphism, and Metamorphism, Dynamic Malware Analysis (DMA) differs from Static Malware Analysis in the sense that it must actually execute the malware in running time or execution time. Debug Execution (like WindDbg, SoftICE) and Run-time Execution are the two most common types of Dynamic Malware Analysis .

It is simple and quick to gain an overview of programmes and evaluate malware that has been observed previously using static analysis. However, analysing malware that use obfuscation, packed, polymorphism, and other methods is very impossible. Malicious software that uses hiding strategies can be detected because programme instructions are executed during dynamic analysis. However, some malware varieties may be aware that they are being examined in sandboxes and virtual environments, causing their true behaviour to be hidden. Static analysis is more accurate for already identified malware. The dynamic analysis is more accurate and successful while dealing with unknown malware.

Malware attacks are the most common type of cybercrime. Malware infects a computer or electronic device and instructs it to carry out the evil task that its author has assigned to it. We may classify malware into several sorts based on the different types of destructive tasks it performs in an infected system.

II. MALWARE TYPES

Virus: Viruses are considered as the mostly seen type of malware.This type of malware will be fetched into the system without the permission of the user or other different programming applications

Worm: This type of malware is also so common.The most difference between the virus and worm is that this type of malware can easily be transmitted to other devices in the connection .

Adware: It is a sort of virus that drives a computer user to inappropriate advertisements. These advertising frequently lead to the download of dangerous programmes or to websites containing sexually explicit content.

Electronic copy available at: https://ssrn.com/abstract=4296051

Spyware: This sort of malware can track the user's activity without their knowledge or agreement once it has infiltrated the system. Collecting keystrokes, data harvesting (financial data, usernames and passwords, and so on) are just a few of the espionage activities.

Rootkit: Its capacity to grant access to data to an intruder with higher permissions than the attacker.For example, give an unauthorised person administrative access.A rootkit is considered as a part of software which allows malware components to have total control over the user's system. Rootkits can infect applications, kernels, hypervisors, and firmware, among other things. Phishing, fraudulent attachments, malware downloads, and corrupted shared folders are all ways to get your information stolen.

Keyloggers: It is a kind of spyware that records the activity of the user known as a keylogger. Keyloggers can be used by businesses to monitor employee behaviour, and by parents to have control on the online activities of their kids. Olympic Vision, a keylogger, has been used in business email compromise (BEC) attacks in the United States, the Middle East, and Asia. When installed for nefarious intentions, keyloggers can be used to Financial information, and other secure informations can be stealed using keyloggers.It can even track the passwords too. Keyloggers can be installed by phishing, social engineering, and malware downloads.

Bots:.Bots are the malwares that can self-propagate and this type of malware can connect back to a central server when employed for some malevolent reasons.Foror malicious purposes, Bots acts as a self-propagating malware such a way that thaey can connect back to a central server.They are widely utilized for security purposes.It is widely used in the area of cyber privacies and securities.These bot attacks were also known as bad bots.

Backdoor: This kind of malwares allows attackers to access the device in a new way. Instead of harming itself, it gives assailants a larger area to assault. Individually, backdoors are rarely used. They frequently happen before other types of malware attacks.

Ransomware: Ransomware is a kind of malware attacks which stops the current user from having a access to their working environment.Current Ransomware detection mechanisms can be of two types: static method and dynamic method.

III. MALWARE ANALYSIS MODELS

There are three types of Malware Analysis: Static, Dynamic, and Memory Malware Analysis,

.

A. Static Analysis

Static Analysis is an analysing approach in which it does not give importance to the execution of the code.It only focuses on the examination of the code without running the entire code.Static analysis finds the error of the code before the execution of the code.This method analyses the code with the certain coding rules and debugs accordingly.

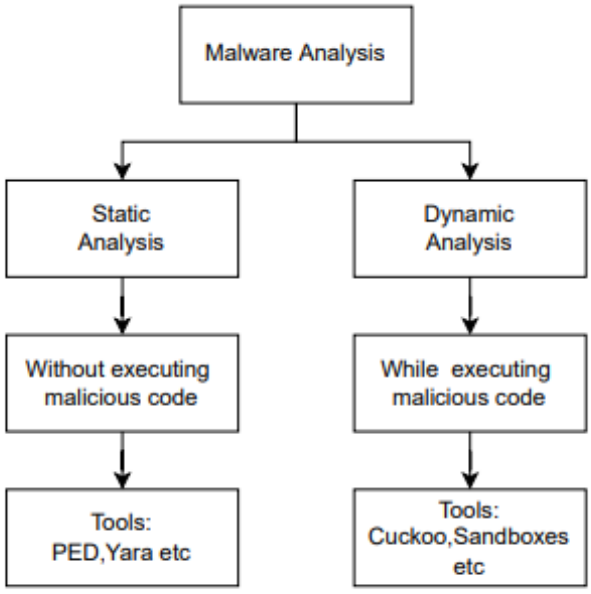

Fig. 1. Malware Analysis Models

B. Dynamic Analysis

Dynamic analysis not only analysis the code by examination but also by executing the malware samples and analysing its performance on the running system based on the output obtained.Dynamic analysis is done to closely find out the error during run time in the real environment.

IV. BACKGROUND

Deep learning is considered as the background.Different deep learning methods used for the classification of malware images includes:

A. Convolutional Neural Network

A Convolutional Neural Network (CNN) is a deep learning model which has a number of convolutional layers. A Convolutional layer has many filters which is used for performing convolutional operations. The filters were given different kernel sizes and the operations were done according to the filter size. Padding can be also included in convolutional layers. Different activation functions can be also used. The outputs resulted from each layer is fed into the very next layer and so on.Since large input sizes is there for the input images where each pixel is a relevant variable,it needs a large number of neurons for execution.

Pooling layer: A Pooling layer is usually placed in between two nearly placed convolution layers in the model. It also have filters of varying sizes and it is termed as pool size. This layer is mainly used to decrease the dimension of the space of representation in order to minimize the number of parameters and thereby it decreases computations in the network. It also used to control overfitting.

Electronic copy available at: https://ssrn.com/abstract=4296051

Fully connected layer: In a fully connected layer, neurons have connections to all nodes in their previous layer and to the next layer, which seems as that of traditional Neural Networks. The convolution and pooling layers were mainly used to extract features from the input images given to the network. The fully connected layer is similar to the simple neural networks and the output of this layer is considered as the final output of the whole architecture.

B. Residual Network

The discipline of computer vision has seen significant changes in past years as a result of the introduction of new technology. As a result of these improvements, computer vision models are now capable of outperforming humans in a variety of tasks such as picture recognition, object detection, face recognition, image categorization, and so on.

The emergence of deep convolutional neural networks, or CNNs, merits special notice in this regard. These networks have been extensively employed for highly accurate visual picture analysis.

It is at this point that the use of ResNet becomes critical.ResNet makes it possible to overcome the challenges of training very deep neural networks. ResNet is an abbreviation for Residual Network. It's a cutting-edge neural network.

1) ResNet 50: ResNet 50 is a type of residual network with 50 layers deep.It has both identity block as welll as convolutional block too. ResNet 50 was developed specifically to address this issue. To improve the accuracy of the models, deep residual nets incorporate residual blocks. Convolutional neural network along with the concept of skip connections is called Residual Network and ResNet 50 is one among them.

The concept of skip connections can be used in two ways.It reduces the problem of vanishing gradients.Both upper levels and lower levels of this network functions equally because they allows the model to learn functions that represents their identity as well.

In short, residual blocks make learning identity functions much easier for the layers. As a result, ResNet boosts the performance of deep neural networks by adding more neural layers while lowering the error rate. To put it another way, skip connections combine the outputs of prior layers with the outputs of stacked layers, allowing for far deeper network training than previously feasible.

2) ResNet 101: ResNet-101 is an another type of residual network which has 101 layers.The ImageNet database can be used to load a pre-trained version of the network that has been used for training different image datasets. The network has been pre-trained to categorise images into almost 1000 different classes.Therefore,it can be used as a background model for the classification of images using the ResNet-101 model, as opposed to ResNet 50. ResNet 101 is a more complicated algorithm that is best suited for large, complex datasets. However, while it allows us to add more layers to the CNNs to perform more difficult computer vision tasks, it comes with its own set of problems. It has been noticed that as the number of added layers increases, training neural networks gets increasingly difficult, and in some cases impossible.

V. RELATED WORKS

The malware detection architecture proposed by Ömer Aslan et al. [1] proposed different methods for feature analysis techniques in the case of malware classification: static way and dynamic way of analysis.There are different methods for analysing the code using static analysisBut dynamic analysis is used to evaluate different moves,mainly making use of private data and restricted API calls.

A. Malicious Code Visualization

Many binary editors and different text editors can be used in order to manipulate binary data. Malware visualisation has been proposed in several studies. Nataraj et al. introduced a new binary texture analysis-based visualisation approach for malware identification. The malware executable code was first transformed into grayscale pictures. The infection was then detected based on the textural qualities of the images.

B. Malware Detection Techniques

The detection and classification of malware has been changed into an image classification problem after the malware has been trandformed into grayscale images. Different algorithms were used to change the weighted factors in the fusion rule in their method. After the execution of this method,the outputs obtained from this model acquired higher accuracy and quality than other models which were practiced before.

There exist a number of techniques to transform binary or hexadecimal code to corresponding images.Here,we use the visualization technique to convert codes to grey scale images.The malware binary file is read in a vector of 8-bits unsigned integers as the first step.Next, using the equation A=$(a0 * 2^0 + a1 * 2^1 + a2 * 2^2 + a3 * 2^3 + a4 * 2^4 + a5 * 2^5 + a6 * 2^6 + a7 * 2^7)$,the respective binary term of each component A=$(a7 + a6 + a5 + a4 + a3 + a2 + a1 + a0)$ is converted into its corresponding decimal value.Atlast,the obtained output vector is reshaped in the form grayscale images.

After that,the Convolutional Neural Network is used for classification of obtained images.The quality of signal can be enhanced and noise can be minimized using the first layer, while the second layer can be used to minimize processing of data while sustaining suitable relevant data.There are a number of completely connected layers that forms a one-dimensional feature from two-dimensional feature that meets the criteria of the classifier.Atlast,the classifier identifies and groups categorize malware images into their corresponding families.

Behaviour of the process developed by Tobiyama et.al. [2] is composed of various activities such as file management and these activities consists of multiple operations.First, the process's behaviour is tracked and recorded in log files. RNN is trained to develop a behavioural language model using these log data. A trained RNN extracts features from log files and converts them to a feature image. Following that,

Electronic copy available at: https://ssrn.com/abstract=4296051

the trained CNN classifies these photos as malware or not. Then, using the classifier output, we calculate the process's malware likelihood.

The convolutional neural networks are mainly used for classification of images, but combining them with embedding improves accuracy by transforming the input vector into a matrix with the same attributes as images, which are stored and processed in a matrix. The approaches like Word2Vec or Glove vectors to categorise tales as true or false, in which all current content in news content is checked or combined with other criteria to retrieve a fixed-size matrix including word mathematical combinations in a statement with set parameters.

Behavioral malware detection proposed by Alsulami et.al. [3] were used to enhance the behaviour of static signature-based techniques. These were considered as less effective against modern polymorphic malware. Behavioral malware categorization tries to go beyond malware detection by identifying a class of malware similar to that of anti-virus providers. Behavioral malware classification approaches capture the behavioural characteristics of running programmes using execution-time features.The second layer here is the convolution layer. A filter of a particular size,particularly, 1-D is added into the second layer. The filter is then passed through the full list by the layer inorder to take out adjacent names of file. Max Pooling is the third layer. The data from the preceding layer is compressed in this layer. Its goal is to boost our model's computing performance and accuracy, as well as the training process.The fourth layer in this architecture is Bidirectional LSTM ,which is a type of recurrent neural network model.

VI. METHODOLOGY

Malware is a malicious programme code which refers to harmful software that can infect a single system or complete network. It takes advantage of weaknesses in the target system, such as a defect in lawful software that can be exploited. Using deep learning algorithms, the malware images from the Malimg dataset are categorised into 25 different classes or families. Here, deep neural network were used to train and classify malware images to corresponding families.This paper mainly proposed two residual network models,namely,ResNet 50 and ResNet 101 for classifying malware samples.In this,9339 malware sample images were taken as input.For training and testing,the available dataset is splited into two categories,ie,70 percent of the sample input is given for training the model and 30 percent of the input sample is taken for testing the new model. First the models of ResNet 50 and ResNet 101 trained using ImageNet dataset were used.Then as the next phase,the new model is built by replacing the top layers of the pre-trained model,ie, fully connected layers and add the new layers as in our proposed model.After taking the weights from the pre-trained model, the newly build model is trained using our malware malimg dataset which consists of 9339 malware images of 25 different malware families.Finally, the new model is trained and malware input images were classified into corresponding 25 different families.

.

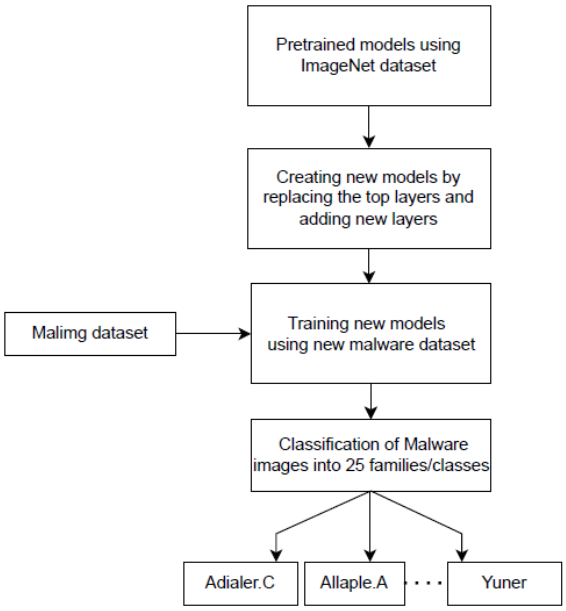

Fig. 2. Proposed Model

A. Dropout

Dropout layers are advantageous in neural network training because they avoid overfitting of the training data. The first batch of training data has a disproportionately strong impact on learning if they aren't present.

B. Batch Normalization

Batch normalisation is a training strategy for extremely deep neural networks that normalises each batch of mini-contributions to a layer.This method improves the learning rate and it reduces the number of training epochs in the neural networks.Batch normalization increases the accuracy of the model as it allows to add more layers in the network.

C. Dense

A dense layer in a neural network is one that is deeply connected to the layer before it, meaning that every neuron in the layer before it is connected to the layer's neurons. This is the most commonly used layer in artificial neural network networks.

D. Flatten

The output obtained from the pooling layer is taken as the input of this layer.This output is fed into a one dimensional array and results in a 1- dimensional results and is given to the fully connected layer for further steps of classification. .

Malware image dataset is trained using ResNet 50 and ResNet 101.Each ResNet 50 and ResNet 101 architectures were trained using two optimizers Adam and RMSprop.

Electronic copy available at: https://ssrn.com/abstract=4296051

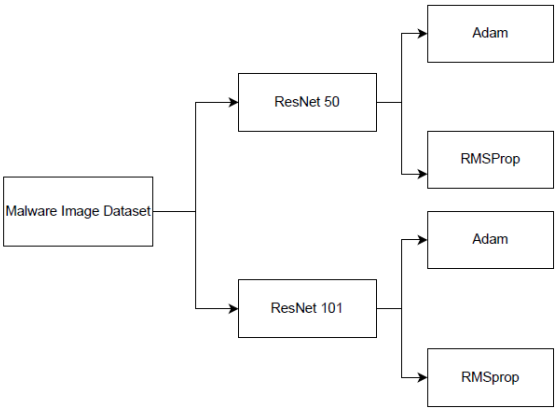

Fig. 3. Design

1) Adam: The Adam optimizer uses gradient descent with momentum .This is used to enhance the speed of the gradient descent algorithm by considering the 'exponentially weighted average' of the gradients. The algorithm's convergence to the minima is accelerated when averages are used.In most of the models,Adam optimizers were used because of its greater performance

2) RMSProp: The RMSprop optimizer is a variant of the gradient descent approach that is based on momentum. The RMSprop optimizer does their oscillations in the horizontal direction by reducing its vertical oscillations.And hence.the learning rate is increased and the algorithm is able to converge in a much faster rate.

.

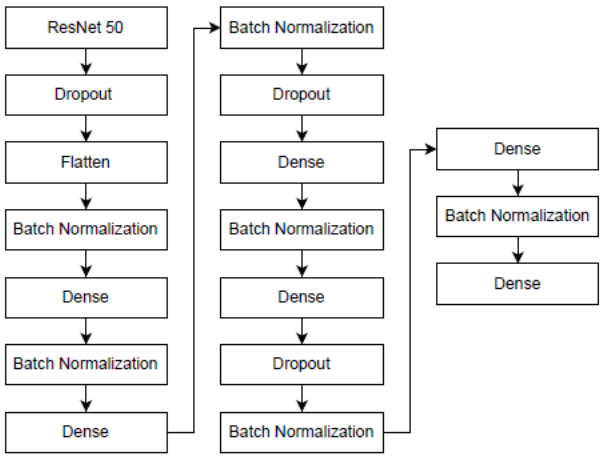

Fig. 4. Block diagram for the proposed model

VII. DATASETS AVAILABLE

Experiments were carried out on three comprehensive datasets. These are Malimg, Microsoft BIG 2015. Details of these three datasets are presented below.Among them, this paper used Malimg dataset for classify malware.

There are 9,339 malware samples in the Malimg collection. Each of the 25 malware classes is represented in the dataset by a malware sample. However,images in each malware class varies in their count in the whole dataset. C2LOP Malex.gen, Lolyda.AA1, Lolyda.AA2, Lolyda.AA3, Lolyda.AT AD, Rbot!gen, Skintrim.N, Swizzor.gen! J, Obfuscator. AD, Rbot!gen, Skintrim.N, Swizzor.gen! Yuner.A, Adialer.C and Agent FYI, Allaple.A, Allaple.L, Alueron.gen!J, Autorun.K, Benign, Benign, Benign, Benign, Benign, Benign, Benign, Benign, Benign, Benign, Benign, Benign, Benign Dialplatform.B, Dontovo.A, Fakerean, Instantaccess, C2LOP.P, C2LOP.gen!g, C2LOP.P, C2LOP.gen!g, C2LOP.P, C2LOP.gen!g, C2LOP.Pare the 25 respective malware classes.

VIII. RESULT ANALYSIS

The experimental analysis shows that ResNet 50 with Adam optimizer has maximum training accuracy compared to ResNet 101 architecture. For easily distinguishable classes and for small sized datasets ResNet 50 performs better than ResNet 101, Here our image dataset is of size 64*64 pixels.So,due to the smaller image size,ResNet 50 functions more accurately than ResNet 101. The Accuracy,F1 score of ResNet 50 and ResNet 101 architectures with Adam and RMSProp optimizers were tabulated.

.

MODELS	OPTIMIZER	ACCURACY	F1-SCORE
ResNet 50	Adam	89.65	89.39
	RMSprop	86.51	85.81
ResNet 101	Adam	82.08	85.70
	RMSprop	81.16	83.33

Fig. 5. Result Analysis

The below graphs clearly depicts the accuracy of ResNet 50 and ResNet 101 model for malware classification using Malimg dataset. From the graph, we can concluded that ResNet 50 model trained with Adam optimizer has more accuracy while comparing with ResNet 50 model trained with RMSProp optimizer. .

.

Electronic copy available at: https://ssrn.com/abstract=4296051

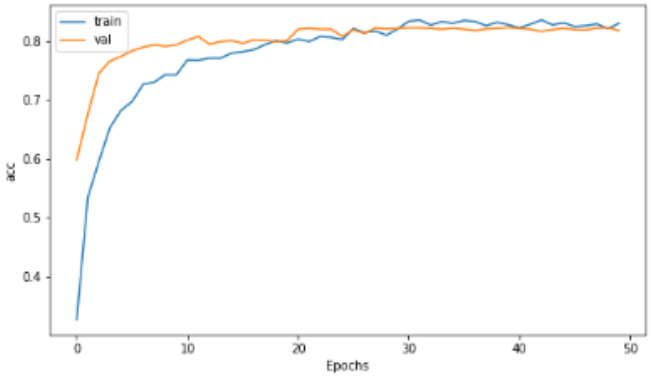

Fig. 6. ResNet 101 accuracy - RMSprop

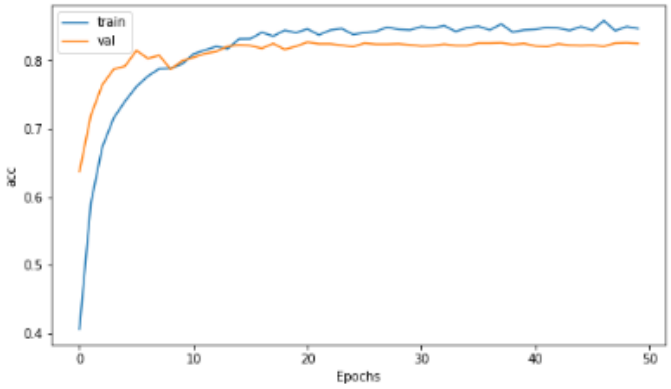

Fig. 7. ResNet 101 accuracy - Adam

.

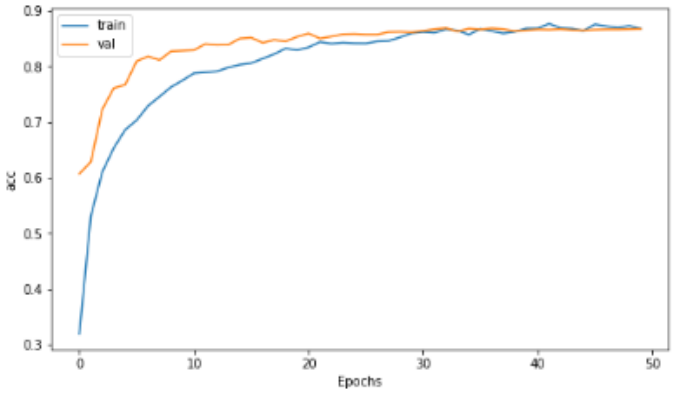

Fig. 8. ResNet 50 accuracy - RMSprop

.

.

Here,we shown the accuracy and loss of ResNet 50 architecture with the two optimizers,ie,Adam and RMSprop.From the graph,it is concluded that the ResNet 50 architecture with Adam optimizer has the maximum accuracy.

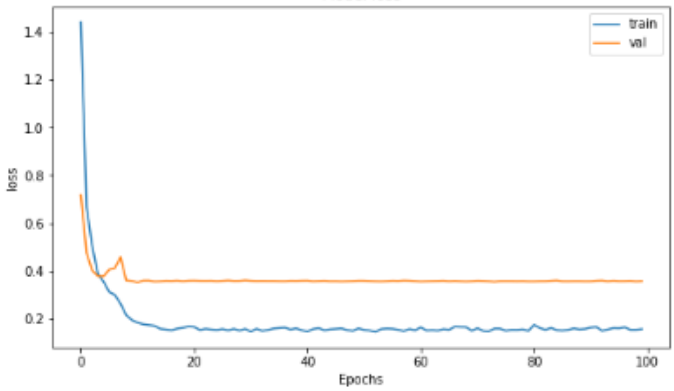

Fig. 9. ResNet 50 loss - Adam

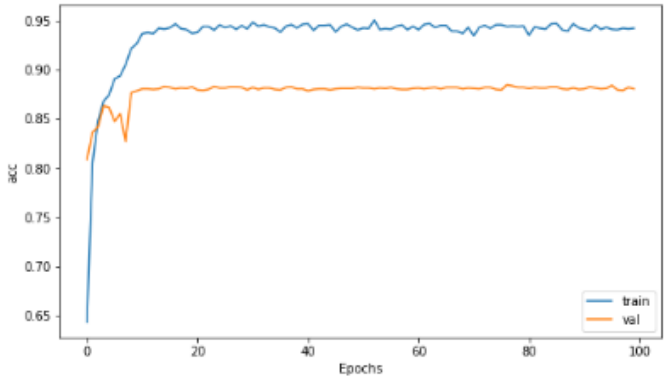

Fig. 10. ResNet 50 accuracy - Adam

IX. CONCLUSION

Malware, often known as malicious software, is a significant hazard to the information technology industry. Deep Neural Networks have lately demonstrated excellent performance in the identification and categorization of malware. In today's world, cyber-crime has become a major problem to people, businesses, and national security systems. Deep Learning (DL) has been used in many safety-oriented contexts for protecting applications due to its rapid evolution and notable accomplishments in a wide range of applications. Intrusion detection, malware categorization and detection, spam detection, and phishing detection are all examples of problems where deep learning approaches have been applied. However, DL can make mistakes owing to internal/external harmful qualities, which might cause problems in our everyday life.This study offers a new approach for detecting harmful cyber-attacks using DL and minimising DL technique misprediction to overcome these limitations.

REFERENCES

[1] Ömer Aslan and Abdullah Asim Yilmaz. A new malware classification framework based on deep learning algorithms. *IEEE Access*, 9:87936–87951, 2021.

Electronic copy available at: https://ssrn.com/abstract=4296051

[2] Shun Tobiyama, Yukiko Yamaguchi, Hajime Shimada, Tomonori Ikuse, and Takeshi Yagi. Malware detection with deep neural network using process behavior. In *2016 IEEE 40th Annual Computer Software and Applications Conference (COMPSAC)*, volume 2, pages 577–582, 2016.

[3] Bander Alsulami and Spiros Mancoridis. Behavioral malware classification using convolutional recurrent neural networks. In *2018 13th International Conference on Malicious and Unwanted Software (MALWARE)*, pages 103–111, 2018.

[4] Chang Hoon Kim, Espoir K. Kabanga, and Sin-Jae Kang. Classifying malware using convolutional gated neural network. In *2018 20th International Conference on Advanced Communication Technology (ICACT)*, pages 1–1, 2018.

[5] Prajna Kotian and Reena Sonkusare. Detection of malware in cloud environment using deep neural network. In *2021 6th International Conference for Convergence in Technology (I2CT)*, pages 1–5, 2021.

[6] Rajvardhan Patil and Wei Deng. Malware analysis using machine learning and deep learning techniques. In *2020 SoutheastCon*, volume 2, pages 1–7, 2020.

[7] Nagababu Pachhala, S. Jothilakshmi, and Bhanu Prakash Battula. A comprehensive survey on identification of malware types and malware classification using machine learning techniques. In *2021 2nd International Conference on Smart Electronics and Communication (ICOSEC)*, pages 1207–1214, 2021.

[8] M. Yeo, Y. Koo, Y. Yoon, T. Hwang, J. Ryu, J. Song, and C. Park. Flow-based malware detection using convolutional neural network. In *2018 International Conference on Information Networking (ICOIN)*, pages 910–913, 2018.

[9] Ümit Köse and Refik Samet. Detection of malware with deep learning method. In *2021 6th International Conference on Computer Science and Engineering (UBMK)*, pages 665–669, 2021.

[10] Sunoh Choi, Sungwook Jang, Youngsoo Kim, and Jonghyun Kim. Malware detection using malware image and deep learning. In *2017 International Conference on Information and Communication Technology Convergence (ICTC)*, pages 1193–1195, 2017.

[11] Ke He and Dong-Seong Kim. Malware detection with malware images using deep learning techniques. In *2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, pages 95–102, 2019.

[12] Zhuojun Ren and Ting Bai. Malware visualization based on deep learning. In *2021 14th International Congress on Image and Signal Processing, BioMedical Engineering and Informatics (CISP-BMEI)*, pages 1–5, 2021.

Electronic copy available at: https://ssrn.com/abstract=4296051